

HUBCITY LAW GROUP
Joseph A. Bahgat (#006502008)
96 Paterson Street
New Brunswick NJ 08901
732 733 2385 x.110
joe@hubcitylawgroup.com
Attorney for Movant

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MALIBU MEDIA, LLC,

Plaintiff;

vs.

JOHN DOE subscriber assigned IP
address 68.38.209.12,

Defendant.

No. 3:14-cv-003945

Judge Michael A. Shipp

Magistrate Judge Douglas E. Arpert

**DEFENDANT DOE'S BRIEF IN SUPPORT
OF MOTION TO QUASH SUBPOENA & MOTION FOR
LEAVE TO PROCEED ANONYMOUSLY**



FACTUAL BACKGROUND

Plaintiff Malibu Media is a pornographic film production company based in California; its business model is primarily based on pornographic copyright infringement litigation, which is predicated on the exploitation of U.S. copyright laws. Indeed, Malibu has filed more than 2,000 lawsuits nationwide, against thousands of defendants, all of which allege the infringement of various pornographic copyrights via BitTorrent. While it is true that copyright infringement is a legitimate basis for a lawsuit, many courts have acknowledged the predatory nature of litigation such as this, and the potentially inappropriate techniques being used by Malibu and other similar plaintiffs in the porn industry, who systematically coerce private individuals into settlements for thousands of dollars to avoid the public shame of being publicly identified & accused of unlawfully downloading pornographic films, and then having to defend such suits in federal court.¹

In 2012, Malibu's practice was to join as many Doe Defendants as possible into a single case, identified only by their subscriber assigned Internet protocol or IP addresses. The complaints alleged that all of the defendants involved in downloading a given file were jointly & severally liable for the resulting infringement. Many courts found that Malibu's system of joining multiple unrelated defendants into a single suit ran afoul of the joinder rules of the Federal Rules of Civil Procedure, which resulted widespread dismissal of these lawsuits. That prompted Malibu to move away from its practice of suing multiple Doe Defendants in a single suit, in favor of bringing suits against single defendants, such as this one.

¹ See, e.g., *Raw Films, Ltd. v. Does 1-32*, No. 11-cv-002939, 2011 WL6840590, at *2, n.5 (N.D.Ga. Dec. 29, 2011) ("The risk of inappropriate settlement leverage is enhanced in a case like this involving salacious and graphic sexual content where a defendant may be urged to resolve a matter at an inflated value to avoid disclosure of the content the defendant was accessing.").

To offset the lost profit margins caused by the increased expense of having to file lawsuits against each Doe Defendant individually, Malibu now targets IP addresses issued in the most affluent zip codes. After filing their complaints, Malibu immediately requests leave to serve third-party subpoenas on the subscribers' Internet Service Provider (ISP). Then, after learning the true identities of the subscribers, Malibu tries to extract larger settlements. The average Malibu settlement demand is \$20,000 per defendant.

Malibu's law firm is Lipscomb, Eisenberg & Baker, of Miami, Florida. Lipscomb, Eisenberg & Baker drafts the pleadings, and then conducts the litigation of these lawsuits using local counsel to file and appear at hearings. Malibu has made a practice out of finding its local counsel by the placing of numerous Internet advertisements & solicitations oftentimes using Craigslist. Using that system, Malibu systematically sues these Doe Defendants for copyright infringement, and then seeks exorbitant settlements.

Indeed, in this case Malibu has already demonstrated the use of such inappropriate procedures, by claiming, in *ex parte* documents, a need to obtain identifying data from an ISP provider (Comcast) "so that Plaintiff may learn Defendant's true identity," yet the information sought includes the email and phone number registered with the ISP.² Release of the email and telephone number is unnecessary for service of process, but can result in harassment of a defendant. The porn-pandering plaintiffs in similar lawsuits have "contacted [the defendants] directly with harassing telephone calls, demanding \$2,900 in compensation to end the litigation."³

² (ECF 5-4, at p. 4.)

³ *Raw Films, Ltd. v. Does 1-32*, No.11-cv-532-JAG, 2011 WL 6182025 (E.D.Va. Oct. 5, 2011).

Malibu claims to own the copyright to 28 works identified in Exhibit B to its complaint.⁴ Some of the films/copyrights at issue in the present litigation have been the subject of litigation in other actions brought by Malibu. Ample evidence exists that Malibu has already concluded hundreds if not thousands of “settlements” with various defendants across the country, many for the exact same copyrights at issue here. As a whole, it is likely that Malibu has already reached the statutory maximum for many of the copyrights it accuses this Doe Defendant of infringing.

Malibu produces and/or distributes pornographic movies available through its X-Art.com website. The movies feature young-looking actors, some of whom are marketed as “teens,” who are engaged in actual & graphic sexual intercourse. Accordingly, Malibu’s movies, including the titles at issue in this lawsuit, are subject to the detailed record-keeping requirements of 18 U.S.C. § 2257. This federal statute was specifically created to prevent child pornography, by ensuring that the porn producers keep and maintain records confirming that the performers it depicts engaging in sexual conduct are at least 18 years old. Violation of § 2257 is a crime, punishable as a felony. Because of the harsh penalties for failing to comply with § 2257 requirements, most smaller porn producers employ professional, third party custodians of records.

Per a legal notice on the X-Art.com website, Malibu doesn’t employ a professional, third-party records custodian. Rather, its custodian of records is identified as “B. Field, 409 W. Olympic Blvd., Suite 501, Los Angeles, CA 90015.” Brigham Field is the Malibu’s founder. Many of the performers in Malibu’s copyrighted works are young females, some of whom are marketed as “teens,” and a substantial number of whom hail from former Soviet-block countries, such as the Czech Republic, Slovakia, Russia, Hungary, and Romania—countries with much less stringent,

⁴ (ECF 1, 1-2.)

and oftentimes ignored, record keeping requirements. On those bases, it is possible the § 2257 records for certain of the pornographic movies at issue in the complaint may be incomplete, deficient, or fabricated.

Plaintiff's technical expert is IPP Limited ("IPP"). IPP operates under a number of aliases including Guardaley and Anti-Piracy Management Company. IPP is responsible for and collecting the computer forensic evidence that serves as the basis for this suit. IPP, operating as Guardaley, was found by a German court to be initially seeding its clients' content onto BitTorrent. If true here as well, and assuming that Movant did download (which he did not) this would constitute an implied license. IPP, operating as Anti-Piracy Management Company, has been under scrutiny in other matters because it has been unwilling or unable to produce forensic evidence. IPP may be responsible for initially seeding plaintiff's content and the purported evidence that serves as the basis for this suit may not exist.

LEGAL ARGUMENT

- 1. This Court should quash the third-party subpoena to Comcast Malibu has not demonstrated the requisite need to be allowed to circumvent the established discovery procedures of the federal courts.**

Malibu got authorization to subpoena Comcast for identifying information about an IP address subscriber, by filing an *ex parte* motion for expedited discovery prior to a Rule 26(f) conference.⁵ There, Malibu faced no adversary to present the prejudices that this Doe Defendant will face as a direct consequence of allowing Malibu to conveniently expedite the discovery process. This Court must balance "the need to provide injured parties with a forum in which they may

⁵ (ECF 5.)

seek redress for grievances” against those of the IP subscriber “without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court’s order to discover their identity.”⁶

This Movant has standing to present this motion to quash, because the movant is party to this action, even though not yet identified.⁷ “[A] party has standing to move to quash a subpoena addressed to another if the subpoena infringes upon the movant’s legitimate interests.” The subpoena issued to Comcast in this case seeks personal identification of the Movant, which required notice to the subscriber pursuant to statute, because Congress has acted to specifically protect this kind private data.⁸ “Parties need only have some personal right or privilege in the information sought to have standing to challenge a subpoena to a third party.”⁹

Malibu’s complaint alleges that its investigation reveals that this Doe Defendant illegally downloaded 28 of its digital “movies” during a period lasting a little longer than one year (March 2013 to May 2014).¹⁰ Despite alleging that this Doe Defendant downloaded 28 complete movies, Malibu admits that only “one or more bits of the digital movie files” listed on the attached Exhibit A were downloaded by its investigator (IPP) from Movant.¹¹ The exchange of one “bit” does not prove infringement of an entire copyrighted work, however, since the computer user may have stopped any further download before the copyrighted work was ever received. As one judge

⁶ *Columbia In. Co. v. SeesCandy.com*, 185 F.R.D. 573, 578 (N.D.Cal 1999).

⁷ *Abels v. State Farm Fire and Cas. Co.*, 770 F.2d 26, 30, n. 3 (3rd Cir. 1985).

⁸ See 47 U.S.C. § 551(2)(B).

⁹ *Third Degree Films, Inc. v. Does 1-108*, No. 11-cv-3007, 2012 WL 669055 (U.S. Dist. Md. 2012).

¹⁰ (See ECF 1-2.)

¹¹ (ECF 1, ¶¶ 19, 22.)



noted about such limited allegations in a similar complaint:

Plaintiffs can only show that someone, using an IP address belonging to the subscriber, was seen online in a torrent swarm. But Plaintiffs did not conduct a sufficient investigation to determine whether that person actually downloaded enough data (or even anything at all) to produce a viewable video. Further, Plaintiffs cannot conclude whether that person spoofed the IP address, is the subscriber of that IP address, or is someone else using that subscriber's Internet access.¹²

That same court explained the problem in more detail in a previous order in the *Ingenuity* case, which criticized the plaintiff's investigation, and the claims in its complaint that were hidden behind a "technical cloak":

The first problem is how Plaintiff concluded that the Defendants actually downloaded the entire copyrighted video, when all Plaintiff has as evidence is a "snapshot observation." This snapshot allegedly shows that the Defendants were downloading the copyrighted work—at least at that moment in time. But downloading a large file like a video takes time; and depending on a user's Internet-connection speed, it may take a long time. In fact, it may take so long that the user may have terminated the download. The user may have also terminated the download for other reasons. To allege copyright infringement based on an IP snapshot is akin to alleging theft based on a single surveillance camera shot: a photo of a child reaching for candy from a display does not automatically mean he stole it. No Court would allow a lawsuit to be filed based on that amount of evidence.

What is more, downloading data via the BitTorrent protocol is not like stealing candy. Stealing a piece of a chocolate bar, however small, is still theft; but copying an encrypted, unusable piece of a video file via the BitTorrent protocol may not be copyright infringement. In the former case, some chocolate was taken; in the latter case, an encrypted, unusable chunk of zeroes and ones. And as part of its *prima facie* copyright claim, Plaintiff must show that Defendants copied the copyrighted work. *Feist Publ'n, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991). If a download was not completed, Plaintiff's lawsuit may be deemed frivolous.

In this case, Plaintiff's reliance on snapshot evidence to establish its copyright infringement claims is misplaced. A reasonable investigation should include evidence showing that Defendants downloaded the entire copyrighted work—or at least a usable portion of a

¹² *Ingenuity 13 LLC v. John Doe*, 2013 WL 1898633, * 3 (C.D. Cal. May 6, 2013).

copyrighted work. Plaintiff has none of this—no evidence that Defendants completed their download, and no evidence that what they downloaded is a substantially similar copy of the copyrighted work. Thus, Plaintiff’s attorney violated Rule 11(b)(3) for filing a pleading that lacks factual foundation.¹³

The Complaint in this case suffers the same crucial flaws, and thus should not support a third party subpoena as early discovery. For instance, the attached Exhibit A to the complaint purports to indicate the “most recent TCP/IP connection between [Plaintiff’s investigator] and Movant’s IP address for each file hash value listed on Exhibit A is included within the column labeled Hit Date UTC.”¹⁴ That exhibit shows that thirty-eight of Plaintiff’s alleged copyright titles were “hit” on a single day – November 30, 2013.¹⁵ Yet many of the “hits” occurred very close in time to each other, some less than one minute, which would make it very unlikely that a full complete copy of a digital movie could have been uploaded from the Defendant’s IP address and then downloaded to the Plaintiff’s investigator in such a brief time period.¹⁶

It is highly improbable that anyone could receive or distribute a full-length movie over the Internet in such a short period of time, given typical Internet speeds in this country. Thus, the Plaintiff’s claims in the complaint in this case. Moreover, the subscriber in control of the IP address being used to distribute Plaintiff’s copyrighted movies, may not be the actual, or even the most likely infringer. An IP address does not identify either the computer or its user, and thus in-



HUBCITY
LAW GROUP

96 Paterson Street
New Brunswick NJ 08901
877 721 9027
www.hubcitylawgroup.com

¹³ *Ingenuity 13 LLC v. John Doe*, No.12-cv-08333, 2013 WL 765102, at *4-5 (C.D.Cal. Feb 7, 2013).

¹⁴ (Compl. ¶ 23, ECF 1, p. 5).

¹⁵ (See ECF 1-1, pp. 2-4).

¹⁶ See, e.g., Complaint, Exhibit A, Doc # 1-1 at pp. 3-4, which indicates two separate movies were “hit” only twenty seconds apart (11/30/2013 17:25:50 to 11/30/2013 17:25:30), or twenty-seven seconds apart (11/30/2013 11:58:15 to 11/30/2013 11:57:48), or fifty-two seconds apart (11/30/2013 05:28:23 to 11/30/2013 05:27:31). A similar pattern is discerned on other dates in Exhibit A.

nocent persons may be dragged into this case if the IP subscriber is disclosed. As one court explained:

[T]he assumption that the person who pays for Internet access at a given location is the same individual who allegedly downloaded a single sexually explicit film is tenuous, and one that has grown more so over time. An IP address provides only the location at which one of any number of computer devices may be deployed, much like a telephone number can be used for any number of telephones. As one introductory guide states:

If you only connect one computer to the Internet, that computer can use the address from your ISP. Many homes today, though, use routers to share a single Internet connection between multiple computers. Wireless routers have become especially popular in recent years, avoiding the need to run network cables between rooms. If you use a router to share an Internet connection, the router gets the IP address issued directly from the ISP. Then, it creates and manages a subnet for all the computers connected to that router.

Thus, it is no more likely that the subscriber to an IP address carried out a particular computer function - here the purported illegal downloading of a single pornographic film - than to say an individual who pays the telephone bill made a specific telephone call.

Indeed, due to the increasingly popularity of wireless routers, it much less likely. While a decade ago, home wireless networks were nearly non-existent, 61% of U.S. homes now have wireless access. Several of the ISPs at issue in this case provide a complimentary wireless router as part of Internet service. As a result, a single IP address usually supports multiple computer devices - which unlike traditional telephones can be operated simultaneously by different individuals. *See U.S. v. Latham*, 2007 WL 4563459, at *4 (D.Nev. Dec.18, 2007). Different family members, or even visitors, could have performed the alleged downloads. Unless the wireless router has been appropriately secured (and in some cases, even if it has been secured), neighbors or passersby could access the Internet using the IP address assigned to a particular subscriber and download the plaintiff's film.¹⁷

In weighing a motion to quash in such cases, a court must balance the need to provide the injured party with a forum against the need to protect IP subscribers from the risk of harassment.

¹⁷ *In re BitTorrent Adult Film Copyright Infringement Cases*, No. 11-3995 DRH, 2012 WL 1570765 (E.D.N.Y. May 1, 2012), report and recommendation adopted *sub nom. Patrick Collins, Inc. v. Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012).

This Court must consider the “expectation of privacy held by . . . innocent users who may be dragged into the case (for example, because they shared an IP address with an alleged infringer).”¹⁸ Any disclosure of information identifying the movant in this case would force them to choose between public embarrassment and a coerced settlement on potentially specious claims. One court noted:

In another Digital Sin case brought by the same counsel as in this case, counsel conceded that there was a high risk of false positive identifications (that is, as many as “30% of the names turned over by the ISPs may not be those of individuals who actually downloaded or shared copyrighted material”) and that there were “horror stories” of harassing and abusive litigation techniques by some law firms. *See Digital Sin*, 2012 WL 263491 at *3. The combination of these factors and the nature of the copyrighted work in this case creates the possibility of undue embarrassment and harm were a Doe defendant’s name to be publicly, but erroneously, linked to the illegal downloading of the plaintiff’s copyrighted work.¹⁹

Copyright owners have a legitimate right to protect their interests by filing a lawsuit against a known infringer. But in recent years there has been a veritable flood of BitTorrent or similar internet copyright infringement lawsuits filed all over the country, and more than one court has found that they provide ample opportunity for abuse by plaintiffs and their lawyers:

Plaintiffs have outmaneuvered the legal system. They’ve discovered the nexus of antiquated copyright laws, paralyzing social stigma, and unaffordable defense costs. And they exploit this anomaly by accusing individuals of illegally downloading a single pornographic video. Then they offer to settle—for a sum calculated to be just below the cost of a bare-bones defense. For these individuals, resistance is futile; most reluctantly pay rather than have their names associated with illegally downloading porn. So now, copyright laws originally designed to compensate starving artists allow starving attorneys in this electronic-

¹⁸ *London-Sire Records, Inc. v. Doe 1*, 542 F. Supp. 2d 153, 179 (D. Mass 2008).

¹⁹ *Digital Sin, Inc. v. Does 1-27*, No. 12-3873, 2012 WL 2036035 (S.D.N.Y. Jun. 6, 2012).

media era to plunder the citizenry.²⁰

Similar concerns have been expressed in cases involving Malibu Media as the plaintiff.²¹

For all of these reasons, Malibu Media's request for discovery of the subscriber in this matter is not justified, especially given the track record in cases like this in which plaintiffs use discovery of personal information to coerce settlements. Therefore, Movant respectfully requests this Court enter an Order quashing the subpoena issued to movant's ISP, Comcast.

Alternatively, Movant's attorney could agree to accept service of the complaint, so there is no need to conduct discovery before the Rule 26(f) conference. The only purported reason Malibu needs to identify Movant immediately is so he or she can be served with process and then participate in this action. If service is accomplished via defendant's counsel, Malibu should not be allowed to conduct any discovery until after the parties confer pursuant to Rule 26(f). If Malibu is unwilling to accomplish service in this alternative manner, then it should not be permitted to use a subpoena to Comcast forcing disclosure of records for the alleged IP subscriber.

2. Even if the Court is not inclined to quash the third-party subpoena, there is no reason why this Doe Defendant should not be allowed to proceed anonymously.

There is a presumption that parties' identities are public information. That presumption and the possible prejudice to the opposing party from concealment can be rebutted, however, by

²⁰ *Ingenuity 13 LLC v. John Doe*, 2013 WL 1898633, * 1 (C.D. Cal. May 6, 2013).

²¹ See, e.g., *Malibu Media, LLC v. Does 1-5*, 2012 WL 2001968, at *2 (S.D.N.Y. June 1, 2012) (there is "risk of receiving coercive phone calls threatening public filings that link [defendants] to alleged illegal copying and distribution of pornographic films, if a settlement fee is not forthcoming"); *Malibu Media v. Does 1-10*, No. 12-cv-3623, 2012 WL 5382304, at *2 (C.D.Cal. June 27, 2012) ("[T]he potential for abuse is very high. The infringed work is a pornographic film. To save himself from embarrassment, even if he is not the infringer, the subscriber will very likely pay the settlement price").



96 Paterson Street
New Brunswick NJ 08901
877 721 9027
www.hubcitylawgroup.com

showing that the harm to the party seeking to proceed anonymously “exceeds the likely harm from concealment.”²² A district court judge has an independent duty to determine whether “exceptional circumstances justify such a departure from the normal method of proceeding in federal courts.”²³ Anonymity has been held to be appropriate when necessary “to preserve privacy in a matter of sensitive and highly personal nature.”²⁴ Moreover, a defendant’s motions to quash subpoenas for the very purpose of protecting their identifying information “should be allowed to proceed anonymously because assessing these preliminary matters without knowing defendants’ identities causes plaintiffs no harm.”²⁵ Finally, it is hard to identify any serious harm to the public in allowing the defendant to proceed anonymously at this early stage of the case.²⁶ In fact, the only reason that Malibu could object to Movant’s request to allow defendant to proceed anonymously is that without the defendant’s actual identity Malibu will be unable to ascertain defendant’s true financial circumstances or net worth (which Malibu would perceive as an impediment to leveraging the maximum possible settlement amount).

Accordingly, there are exceptional and compelling circumstances to allow this Doe Defendant to proceed anonymously, at least in such a preliminary matter as a motion to quash or a motion seeking a protective order.

²² *Doe v. City of Chicago*, 360 F.3d 667, 669 (7th Cir. 2004).

²³ *Doe v. Blue Cross & Blue Shield United of Wisconsin*, 112 F.3d 869, 872 (7th Cir. 1997).

²⁴ *Does I thru XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1068 (9th Cir. 2000); *Third Degree Films v. Does 1-3577*, No. 11-02768 LB, 2011 WL 5374569 (N.D.Cal. Nov. 4, 2011) (“An allegation that an individual illegally downloaded adult entertainment likely goes to matters of a sensitive and highly personal nature, including one’s sexuality.”).

²⁵ *CineTel Films, Inc. v. Does 1-1,052*, 853 F. Supp. 2d 545, 548, n.2 (D.Md. 2012).

²⁶ See *Sunlust Pictures, LLC v. Does 1-75*, No. 12-1546, 2012 WL 3717768, at *5 (N.D.Ill. Aug. 27, 2012) (“because Doe (as a defendant) has not purposefully availed himself of the courts, the public’s interest in knowing his identity is weaker”).

Respectfully submitted,

7-Nov-2014

By: 
Joseph A. Bahgat (#006502008)



CERTIFICATE OF SERVICE

I certify that on the Seventh Day of November 2014, a true and correct copy of the foregoing brief was electronically filed using the CM/ECF system, and that counsel of record was/were served with notice of the same.


JOSEPH A. BAHGAT (\$006502008)

